

An Algebra of Pure Quantum Programming

Thorsten Altenkirch¹ Jonathan Grattage¹

The University of Nottingham, UK

Juliana K. Vizzotto²

Federal University of Rio Grande do Sul, Brazil

Amr Sabry³

Indiana University, USA

Abstract

We develop a sound and complete equational theory for the functional quantum programming language QML. The soundness and completeness of the theory are with respect to the previously-developed denotational semantics of QML. The completeness proof also gives rise to a normalisation algorithm following the *normalisation by evaluation* approach. The current work focuses on the pure fragment of QML omitting measurements.

Key words: quantum programming, completeness, normalisation

1 Introduction

The language QML was previously introduced by the first two authors [AG04]. Its semantics is inspired by the denotational semantics of classical reversible computations. This previous work provides a semantic foundation for reasoning about quantum programs by mapping them to their denotations.

The natural next step is to develop reasoning principles on QML programs themselves which avoid the detour via the denotational semantics. For example, given the following QML definition of the Hadamard gate:

$$\begin{aligned} H\ x &= \text{if}^\circ\ x \\ &\quad \text{then } (false + (-1) * true) \\ &\quad \text{else } (false + true) \end{aligned}$$

¹ Email: {txa,jjg}@cs.nottingham.ac.uk

² Email: jkv@inf.ufrgs.br

³ Email: sabry@indiana.edu

We would like to verify that $H (H x)$ is observationally equivalent to x , using a derivation like:

$$\begin{aligned}
 H (H x) &= \mathbf{if}^\circ (x \\
 &\quad \mathbf{then} (false + (-1) * true) \\
 &\quad \mathbf{else} (false + true)) \\
 &\quad \mathbf{then} (false + (-1) * true) \\
 &\quad \mathbf{else} (false + true) \\
 &\quad \text{-- by commuting conversion for } \mathbf{if}^\circ \\
 &= \mathbf{if}^\circ x \\
 &\quad \mathbf{then} \mathbf{if}^\circ (false + (-1) * true) \\
 &\quad \quad \mathbf{then} (false + (-1) * true) \\
 &\quad \quad \mathbf{else} (false + true) \\
 &\quad \mathbf{else} \mathbf{if}^\circ (false + true) \\
 &\quad \quad \mathbf{then} (false + (-1) * true) \\
 &\quad \quad \mathbf{else} (false + true) \\
 &\quad \text{-- by } \mathbf{if}^\circ \\
 &= \mathbf{if}^\circ x \\
 &\quad \mathbf{then} (false - false + true + true) \\
 &\quad \mathbf{else} (false + false + true - true) \\
 &\quad \text{-- by simplification and normalisation} \\
 &= \mathbf{if}^\circ x \mathbf{ then } true \mathbf{ else } false \\
 &\quad \text{-- by } \eta\text{-rule for } \mathbf{if}^\circ \\
 &= x
 \end{aligned}$$

It is relatively easy to develop *some* set of sound equational principles. Inspired by equivalences on classical computations, one may hypothesise that certain equations should hold and simply verify that both sides of the equation have the same denotation.

Given, however, that QML is based on a first-order functional language with finite types, it should be possible to also develop a *complete* set of equivalences that totally capture denotational equivalence. Technically, one can prove completeness of the equational semantics by “inverting” the denotational meaning function. The construction is subtle in parts. We present it first in the context of the classical sublanguage of QML, and then extend it to deal with quantum data and control.

The paper is thus organised as follows. We begin with an informal review of QML in Section 3. In Section 4, we present the denotational semantics of the classical sublanguage of QML, and present a system of equations that is sound with respect to the denotational semantics. We then show that this set of equations is complete in Section 5. Section 6 repeats the development for the quantum constructs. Section 7 concludes.

2 Related work

Peter Selinger’s influential paper [Sel04] introduces a single-assignment (essentially functional) quantum programming language, which is based on the separation of *classical control* and *quantum data*. This language combines high-level classical structures with operations on quantum data, and has a clear mathematical semantics in the form of superoperators. Quantum data can be manipulated by using unitary operators or by measurement, which can effect the classical control flow.

Recently, Selinger and Valiron [SV05] have presented a functional language based on the same *classical control* and *quantum data* paradigm. Selinger and Valiron’s approach is in some sense complementary to ours: they use an affine type system (no contraction), while we use a strict system (no weakening). The lack of contraction is justified by the no-cloning property of quantum states. However, this does not apply to our approach, since we model contraction by sharing not by copying — this is also used in the calculus of Arrighi and Dowek [AD04].

Andre van Tonder [vT03a,vT03b] has proposed a quantum λ -calculus incorporating higher order programs, but no measurements. He also suggests an equational theory for strict (higher order) computations, but shows neither completeness nor normalisation.

3 QML Syntax and Examples

The QML terms consist of those of a first-order functional language, extended with quantum data and quantum control. The full language also includes quantum measurement, which we do not consider in this paper. The syntax of terms is the following:

$$\begin{array}{ll}
 (\text{Variables}) & x, y, \dots \in \text{Vars} \\
 (\text{Prob. amplitudes}) & \kappa, \iota, \dots \in \mathbb{C} \\
 (\text{Patterns}) & p, q ::= x \mid (x, y) \\
 (\text{Terms}) & t, u, e ::= x \mid () \mid (t, u) \\
 & \mid \text{let } p = t \text{ in } u \\
 & \mid \text{if}^\circ t \text{ then } u \text{ else } u' \\
 & \mid \text{false} \mid \text{true} \mid \overrightarrow{0} \mid \kappa * t \mid t + u
 \end{array}$$

The classic sublanguage consists of variables, **let**-expressions, unit, pairs, booleans, and conditionals. Quantum data is modelled using the constructs $\kappa * t$, $\overrightarrow{0}$, and $t + u$. The term $\kappa * t$ where κ is a complex number associates the *probability amplitude* κ with the term t . It is convenient to have a special constant $\overrightarrow{0}$ for terms with probability amplitude zero. The term $t + u$ is a quantum *superposition* of t and u . Quantum superpositions are first-class values: when used as the first subexpression of a conditional, they turn the conditional into a *quantum control* construct. For example, **if**[°] ($\text{true} + \text{false}$) **then** t **else** u evaluates both t and u and combines their results in a quantum superposition.

3.1 Examples

To give further intuition about the semantics of QML, we consider a few more interesting examples. In the examples, we allow the definition and use of “global” function symbols. Adding such definitions to the formalism is possible but tedious, so we keep them at an informal meta-level.

The following three functions correspond to simple rotations on qubits:

$$\begin{aligned} \text{qnot } x &= \text{if}^\circ x \text{ then } \text{false} \text{ else } \text{true} \\ \text{had } x &= \text{if}^\circ x \text{ then } ((-1) * \text{true} + \text{false}) \text{ else } (\text{true} + \text{false}) \\ z \ x &= \text{if}^\circ x \text{ then } (i * \text{true}) \text{ else } \text{false} \end{aligned}$$

The first is the quantum version of boolean negation: it behaves as usual when applied to classical values but it also applies to quantum data. Evaluating $\text{qnot } (\kappa * \text{false} + \iota * \text{true})$ swaps the probability amplitudes associated with false and true . The second function represents the fundamental *Hadamard* matrix, and the third represents the *phase* gate.

The function:

$$\begin{aligned} \text{cnot } c \ x &= \text{if}^\circ c \\ &\quad \text{then } (\text{true}, \text{qnot } x) \\ &\quad \text{else } (\text{false}, x) \end{aligned}$$

is the conditional-not operation, which behaves as follows: if the control qubit c is true it negates the second qubit x ; otherwise it leaves it unchanged. When the control qubit is in some superposition of true and false , the result is a superposition of the two pairs resulting from the evaluation of each branch of the conditional. For example, evaluating $\text{cnot } (\text{false} + \text{true}) \ \text{false}$ produces the *entangled* pair $(\text{false}, \text{false}) + (\text{true}, \text{true})$.

3.2 Copying and Discarding Quantum Data

To motivate the main aspects of the type system in the next section, we examine in detail the issues related to copying and discarding quantum data.

A simple example where quantum data appears to be copied, in violation of the *no-cloning* theorem [NC00], is:

$$\begin{aligned} &\text{let } x = \text{false} + \text{true} \\ &\text{in } (x, x) \end{aligned}$$

As the formal semantics of QML clarifies, this expression does not actually clone quantum data; rather it *shares* one copy of the quantum data. With this interpretation, one can freely duplicate variables bound to quantum data. When translated to the type system, this means that the type system imposes no restrictions on the use of the structural rule of *contraction*.

Discarding variables bound to quantum data is however problematic. Consider the expression:

$$\begin{aligned} &\text{let } (x, y) = (\text{false}, \text{false}) + (\text{true}, \text{true}) \\ &\text{in } x \end{aligned}$$

where the quantum data bound to y is discarded. According to both the phys-

ical interpretations of quantum computation, and the semantics of QML, this corresponds to a *measurement* of y . Since measurement is semantically quite complicated to deal with, we insist that it should be represented explicitly. The language we consider in this paper lacks the explicit constructs for measurement so we reject the expression above. This means that the structural rule of *weakening* is never allowed in situations where information may be lost.

4 The Classical Sublanguage

By the classical sublanguage, we mean the subset of terms excluding quantum superpositions and hence quantum control.

4.1 Type System

The main rôle of the type system is to control the use of variables. The typing rules of QML are based on strict linear logic, where contractions are implicit and weakenings are not allowed when they correspond to information loss. As explained in the previous section, weakenings correspond to measurements, which are not supported in the subset of the language discussed in this paper.

We use σ, τ, ρ to vary over QML types which are given by the following grammar:

$$\sigma = \mathcal{Q}_1 \mid \mathcal{Q}_2 \mid \sigma \otimes \tau$$

As apparent from the grammar, QML types are first-order and finite: there are no higher-order types and no recursive types. The only types we can represent are the types of collections of qubits.

Typing contexts (Γ, Δ) are given by:

$$\Gamma = \bullet \mid \Gamma, x : \sigma$$

where \bullet stands for the empty context, but is omitted if the context is non-empty. For simplicity we assume that every variable appears at most once. Contexts correspond to functions from a finite set of variables to types. We introduce the operator \otimes , mapping pairs of contexts to contexts:

$$\begin{aligned} (\Gamma, x : \sigma) \otimes (\Delta, x : \sigma) &= (\Gamma \otimes \Delta), x : \sigma \\ (\Gamma, x : \sigma) \otimes \Delta &= (\Gamma \otimes \Delta), x : \sigma \text{ if } x \notin \text{dom}(\Delta) \\ \bullet \otimes \Delta &= \Delta \end{aligned}$$

This operation is partial: it is only well-defined if the two contexts do not assign different types to the same variable. Whenever we use this operator we implicitly assume that it is well-defined.

Figure 1 presents the rules for deriving valid typing judgements $\Gamma \vdash t : \sigma$. The only variables that may be dropped from the context are the ones of type \mathcal{Q}_1 which, by definition, carry no information. Otherwise the type system forces every variable in the context to be used (perhaps more than once if it is shared).

$\frac{}{x : \sigma \vdash x : \sigma} \text{var}$	$\frac{\Gamma \vdash t : \sigma \quad \Delta, x : \sigma \vdash u : \tau}{\Gamma \otimes \Delta \vdash \text{let } x = t \text{ in } u : \tau} \text{let}$
$\frac{}{\bullet \vdash () : \mathcal{Q}_1} \text{unit}$	$\frac{\Gamma \vdash t : \sigma \quad \Delta \vdash u : \tau}{\Gamma \otimes \Delta \vdash (t, u) : \sigma \otimes \tau} \otimes\text{-intro}$
$\frac{\Gamma \vdash t : \sigma \otimes \tau \quad \Delta, x : \sigma, y : \tau \vdash u : \rho}{\Gamma \otimes \Delta \vdash \text{let } (x, y) = t \text{ in } u : \rho} \otimes\text{-elim}$	
$\frac{}{\bullet \vdash \text{false} : \mathcal{Q}_2} \text{f-intro}$	$\frac{}{\bullet \vdash \text{true} : \mathcal{Q}_2} \text{t-intro}$
$\frac{\Gamma \vdash c : \mathcal{Q}_2 \quad \Delta \vdash t, u : \sigma}{\Gamma \otimes \Delta \vdash \text{if}^\circ c \text{ then } t \text{ else } u : \sigma} \text{if}^\circ$	$\frac{\Gamma, x : \mathcal{Q}_1 \vdash t : \sigma}{\Gamma \vdash t : \sigma} \text{wk-unit}$

Fig. 1. Typing classical terms

4.2 The Category of Typed Terms

The set of typed terms can be organised in an elegant categorical structure, which facilitates the proofs later. The objects of the category are contexts; the homset between the objects Γ and Δ , denoted $\text{Tm } \Gamma \Delta$, consists of all the terms t such that $\Gamma \vdash t : |\Delta|$ where $|\Delta|$ views the context Δ as a type. This latter map is naturally defined as follows:

$$|\bullet| = \mathcal{Q}_1$$

$$|\Gamma, x : \sigma| = |\Gamma| \otimes \sigma$$

For each context Γ , the identity $1_\Gamma \in \text{Tm } \Gamma \Gamma$ is defined as follows:

$$1_\bullet = ()$$

$$1_{\Gamma, x : \sigma} = (1_\Gamma, x)$$

To express composition, we first define:

$$\text{let}^* \bullet = u \text{ in } t \quad \equiv \quad t$$

$$\text{let}^* \Gamma, x : \sigma = u \text{ in } t \quad \equiv \quad \text{let } (x_r, x) = u \text{ in let}^* \Gamma = x_r \text{ in } t$$

Given $d \in \text{Tm } \Delta \Gamma$ and $e \in \text{Tm } \Gamma \Theta$, the composition $e \circ d \in \text{Tm } \Delta \Theta$ is given by the term $\text{let}^* \Gamma = d \text{ in } e$.

4.3 Semantics

The intention is to interpret every type σ and every context Γ as finite sets $\llbracket \sigma \rrbracket$ and $\llbracket \Gamma \rrbracket$, and then interpret a judgement $\Gamma \vdash t : \sigma$ as a function $\llbracket \Gamma \vdash t : \sigma \rrbracket \in \llbracket \Gamma \rrbracket \rightarrow \llbracket \sigma \rrbracket$.

In the classical case, the type \mathcal{Q}_2 is simply the type of booleans; the types are interpreted as follows:

$$\begin{aligned}\llbracket \mathcal{Q}_1 \rrbracket &= \{0\} \\ \llbracket \mathcal{Q}_2 \rrbracket &= \{0, 1\} \\ \llbracket \sigma \otimes \tau \rrbracket &= \llbracket \sigma \rrbracket \times \llbracket \tau \rrbracket\end{aligned}$$

We use the abbreviation $\llbracket \Gamma \rrbracket$ for $\llbracket \llbracket \Gamma \rrbracket \rrbracket$.

The meaning function is defined in Figure 2 by induction over the structure of type derivations. It uses the following auxiliary maps:

- $id : S \rightarrow S$ defined by $id(a) = a$
- $id^* : S \rightarrow \llbracket \mathcal{Q}_1 \rrbracket \times S$ and its inverse id_* defined by $id^*(a) = (0, a)$ and $id_*(0, a) = a$
- For $a \in S$, the family of constant functions $const\ a : \llbracket \mathcal{Q}_1 \rrbracket \rightarrow S$ defined by $(const\ a)(0) = a$.
- $\delta : S \rightarrow (S, S)$ defined by $\delta(a) = (a, a)$
- $swap : S \times T \rightarrow T \times S$ defined by $swap(a, b) = (b, a)$. We will usually implicitly use $swap$ to avoid cluttering the figures with maps which just re-shuffle values.
- For any two functions $f \in S_1 \rightarrow T_1$ and $g \in S_2 \rightarrow T_2$, the function $(f \times g) : (S_1 \times S_2) \rightarrow (T_1 \times T_2)$ is defined as usual:

$$(f \times g)(a, b) = (f\ a, g\ b)$$

- $\delta_{\Gamma, \Delta} : \llbracket \Gamma \otimes \Delta \rrbracket \rightarrow \llbracket \Gamma \rrbracket \times \llbracket \Delta \rrbracket$. This map is defined by induction on the definition of $\Gamma \otimes \Delta$ as follows:

$$\delta_{\Gamma, \Delta} = \begin{cases} \delta_{\Gamma', \Delta'} \times \delta & \text{if } \Gamma = \Gamma', x : \sigma \text{ and } \Delta = \Delta', x : \sigma \\ \delta_{\Gamma', \Delta} \times id & \text{if } \Gamma = \Gamma', x : \sigma \text{ and } x \notin \text{dom}(\Delta) \\ id^* & \text{if } \Gamma = \bullet \end{cases}$$

Intuitively, the map $\delta_{\Gamma, \Delta}$ takes an incoming environment for an expression, creates shared copies of the appropriate values, and rearranges them (the shuffling is implicit and not shown in the above definition) into two environments that are then passed to the subexpressions.

- For any two functions $f, g \in S \rightarrow T$, we define the conditional $f|g \in (\llbracket \mathcal{Q}_2 \rrbracket \times S) \rightarrow T$ as follows:

$$\begin{aligned}(f|g)\ (1, a) &= f\ a \\ (f|g)\ (0, a) &= g\ a\end{aligned}$$

$$\begin{aligned}
 \llbracket \bullet \vdash () : \mathcal{Q}_1 \rrbracket &= \text{const } 0 \\
 \llbracket \bullet \vdash \text{false} : \mathcal{Q}_2 \rrbracket &= \text{const } 0 \\
 \llbracket \bullet \vdash \text{true} : \mathcal{Q}_2 \rrbracket &= \text{const } 1 \\
 \llbracket x : \sigma \vdash x : \sigma \rrbracket &= \text{id}_* \\
 \llbracket \Gamma \otimes \Delta \vdash \text{let } x = t \text{ in } u : \tau \rrbracket &= g \circ (f \times \text{id}) \circ \delta_{\Gamma, \Delta} \\
 &\quad \text{where } f = \llbracket \Gamma \vdash t : \sigma \rrbracket \\
 &\quad \quad g = \llbracket \Delta, x : \sigma \vdash u : \tau \rrbracket \\
 \llbracket \Gamma \otimes \Delta \vdash (t, u) : \sigma \otimes \tau \rrbracket &= (f \times g) \circ \delta_{\Gamma, \Delta} \\
 &\quad \text{where } f = \llbracket \Gamma \vdash t : \sigma \rrbracket \\
 &\quad \quad g = \llbracket \Delta \vdash u : \tau \rrbracket \\
 \llbracket \Gamma \otimes \Delta \vdash \text{let } (x, y) = t \text{ in } u : \rho \rrbracket &= g \circ (f \times \text{id}) \circ \delta_{\Gamma, \Delta} \\
 &\quad \text{where } f = \llbracket \Gamma \vdash t : \sigma \otimes \tau \rrbracket \\
 &\quad \quad g = \llbracket \Delta, x : \sigma, y : \tau \vdash u : \rho \rrbracket \\
 \llbracket \Gamma \otimes \Delta \vdash \text{if}^\circ c \text{ then } t \text{ else } u : \sigma \rrbracket &= (g|h) \circ (f \times \text{id}) \circ \delta_{\Gamma, \Delta} \\
 &\quad \text{where } f = \llbracket \Gamma \vdash c : \mathcal{Q}_2 \rrbracket \\
 &\quad \quad g = \llbracket \Delta \vdash t : \sigma \rrbracket \\
 &\quad \quad h = \llbracket \Delta \vdash u : \sigma \rrbracket \\
 \llbracket \Gamma \vdash t : \sigma \rrbracket &= f \circ \text{id}^* \\
 &\quad \text{where } f = \llbracket \Gamma, x : \mathcal{Q}_1 \vdash t : \sigma \rrbracket
 \end{aligned}$$

Fig. 2. Meaning of classical derivations

4.4 Equational Theory

We present the equational theory for the classical sublanguage and then show its soundness and completeness. The equations refer to a set of syntactic values defined as follows:

$$val \in \text{Val}^C ::= x \mid () \mid \text{false} \mid \text{true} \mid (val_1, val_2)$$

Definition 4.1 The *classical equations* are grouped in four categories.

- **let-equation**

$$\text{let } p = val \text{ in } u \quad \equiv \quad u [val / p]$$

- **β -equations**

$$\text{let } (x, y) = (t, u) \text{ in } e \quad \equiv \quad \text{let } x = t \text{ in let } y = u \text{ in } e$$

$$\text{if}^\circ \text{false then } t \text{ else } u \quad \equiv \quad u$$

$$\text{if}^\circ \text{true then } t \text{ else } u \quad \equiv \quad t$$

- **η -equations**

$()$	\equiv	t -- if $t:Q_1$
$\text{let } x = t \text{ in } x$	\equiv	t
$\text{let } (x, y) = t \text{ in } (x, y)$	\equiv	t
$\text{if}^\circ t \text{ then } true \text{ else } false$	\equiv	t
• Commuting conversions		
$\text{let } p = t \text{ in let } q = u \text{ in } e$	\equiv	$\text{let } q = u \text{ in let } p = t \text{ in } e$
$\text{let } p = \text{if}^\circ t$	\equiv	$\text{if}^\circ t$
$\quad \text{then } u_0$		$\text{then let } p = u_0 \text{ in } e$
$\quad \text{else } u_1$		$\text{else let } p = u_1 \text{ in } e$
$\text{in } e$		

We write $\Gamma \vdash t \equiv u : \sigma$ if $\Gamma \vdash t, u : \sigma$ and the equation $t \equiv u$ is derivable at the type σ .

Lemma 4.2 (Soundness) *The equational theory is sound: if $\Gamma \vdash t \equiv u : \sigma$ then the functions $\llbracket \Gamma \vdash t : \sigma \rrbracket$ and $\llbracket \Gamma \vdash u : \sigma \rrbracket$ are extensionally equal.*

5 Completeness of the Classical Theory

The equational theory is *complete* in a strong technical sense: as we prove in the remainder of the section, any equivalence implied by the semantics is derivable in the theory. The proof technique is based on current work by the first author with Tarmo Uustalu [AU04]. The proof we present extends and simplifies the method presented in that work.

5.1 Proof Technique

The ultimate goal is to prove the following statement.

Proposition 5.1 (Completeness) *If $\llbracket \Gamma \vdash t : \sigma \rrbracket$ and $\llbracket \Gamma \vdash u : \sigma \rrbracket$ are extensionally equal, then we can derive $\Gamma \vdash t \equiv u : \sigma$.*

In order to prove this statement, we define a function q_Γ^σ which inverts evaluation by producing a canonical syntactical representative. In fact, we define the function q_Γ^σ such that it maps a denotation $\llbracket \Gamma \vdash t : \sigma \rrbracket$ to the normal form of t .

Definition 5.2 The *normal form* of t is given by $\text{nf}_\Gamma^\sigma(t) = q_\Gamma^\sigma(\llbracket \Gamma \vdash t : \sigma \rrbracket)$.

The normal form is well-defined: given an equation $\Gamma \vdash t \equiv u : \sigma$, we know by soundness that $\llbracket \Gamma \vdash t : \sigma \rrbracket$ is extensionally equal $\llbracket \Gamma \vdash u : \sigma \rrbracket$ and hence we get that $\text{nf}_\Gamma^\sigma(t) = \text{nf}_\Gamma^\sigma(u)$. If we can now prove that the syntactic theory can prove that every term is equal to its normal form, then we can prove the main completeness result. Indeed given the following lemma, we can prove completeness.

Lemma 5.3 (Inversion) *The equation $\Gamma \vdash \text{nf}_\Gamma^\sigma(t) \equiv t : \sigma$ is derivable.*

Proof of Proposition 5.1 (Completeness) We have:

$$\begin{aligned} \Gamma \vdash t &\equiv q_{\Gamma}^{\sigma}[\Gamma \vdash t : \sigma] : \sigma && \text{by inversion} \\ \Gamma \vdash q_{\Gamma}^{\sigma}[\Gamma \vdash t : \sigma] &\equiv q_{\Gamma}^{\sigma}[\Gamma \vdash u : \sigma] : \sigma && \text{by assumption} \\ \Gamma \vdash q_{\Gamma}^{\sigma}[\Gamma \vdash u : \sigma] &\equiv u : \sigma && \text{by inversion} \end{aligned}$$

□

To summarise we can establish completeness by defining a function q_{Γ}^{σ} that inverts evaluation and that satisfies Inversion Lemma 5.3.

5.2 Adequacy

We begin by defining a family of functions q^{σ} (“quote”) which invert the evaluation of *closed* terms and prove a special case of the inversion lemma for closed terms, called *adequacy*. These functions and the adequacy result are then used in the next section to invert the evaluation of open terms and prove the general inversion lemma.

Definition 5.4 The *syntactic representations of denotations* is given by:

$$q^{\sigma} \in \llbracket \sigma \rrbracket \rightarrow \text{Val}^C \sigma$$

defined by induction over σ :

$$\begin{aligned} q^{\mathcal{Q}_1} 0 &= () \\ q^{\mathcal{Q}_2} 0 &= \text{false} \\ q^{\mathcal{Q}_2} 1 &= \text{true} \\ q^{\sigma \otimes \tau} (a, b) &= (q^{\sigma} a, q^{\tau} b) \end{aligned}$$

The version of the inversion lemma for closed terms is called *adequacy*. It guarantees that the equational theory is rich enough to equate every closed term with its final observable value.

Lemma 5.5 (Adequacy) *The equation $\vdash q^{\sigma}(\llbracket \vdash t : \sigma \rrbracket 0) \equiv t : \sigma$ is derivable.*

Proof sketch. During the proof of such a statement we encounter open terms that must be closed before they are “quoted.” So in fact the statement to prove by induction is the following:

$$\text{If } g \in \llbracket \Gamma \rrbracket \text{ then } \vdash q^{\sigma}(\llbracket \Gamma \vdash t : \sigma \rrbracket g) \equiv \mathbf{let}^* \Gamma = q^{\Gamma} (g) \mathbf{in } t : \sigma$$

□

5.3 Inverting Evaluation

As explained earlier, the main ingredient of the proof of completeness is the function q_{Γ}^{σ} which inverts evaluation. To understand the basic idea of how the inverse of evaluation is defined, consider the following example. Let Γ be the

environment $x : (\mathcal{Q}_2 \otimes \mathcal{Q}_2), y : \mathcal{Q}_2$ and let $f \in \llbracket \Gamma \rrbracket \rightarrow \llbracket \mathcal{Q}_2 \rrbracket$. To find a syntactic term corresponding to f , we proceed as follows:

- flatten all the products by introducing intermediate names; this produces an updated environment $\Gamma' = x_1 : \mathcal{Q}_2, x_2 : \mathcal{Q}_2, y : \mathcal{Q}_2$, and an updated semantic function f' such that:

$$f' ((((), x_1), x_2), y) = f ((((), (x_1, x_2))), y)$$

- enumerate all possible values for the variables, and apply f' to each enumeration to produce a result in the set $\llbracket \mathcal{Q}_2 \rrbracket$. For example, it could be the case that $f ((((), (1, 1)), 1) = 0$. The result of each enumeration can be inverted to a syntactic term using q^σ from Definition 5.4.
- Put things together using nested conditions representing all the possible values for the input variables. In the example we are considering, we get:

```

let (x1, x2) = x
in if° x1
  then if° x2
    then if° y then false
    else ...
  else ...
else ...
    
```

The idea is formalised in the following definition.

Definition 5.6 The function

$$q_\Gamma^\sigma \in (\llbracket \Gamma \rrbracket \rightarrow \llbracket \sigma \rrbracket) \rightarrow \text{Tm } \Gamma \sigma$$

for *inverting evaluation* is defined by analysing the context:

$$\begin{aligned}
 q_\bullet^\sigma(f) &= q^\sigma(f(0)) \\
 q_{\Gamma, x: \mathcal{Q}_1}^\sigma(f) &= q_\Gamma^\sigma(h) \quad \text{where } h(g) = f(g, 0) \\
 q_{\Gamma, x: \mathcal{Q}_2}^\sigma(f) &= (\text{if}^\circ x \text{ then } q_\Gamma^\sigma(h_1) \text{ else } q_\Gamma^\sigma(h_0)) \\
 &\quad \text{where } h_i(g) = f(g, i) \text{ for } i \in \{0, 1\} \\
 q_{\Gamma, x: (\tau_1 \otimes \tau_2)}^\sigma(f) &= (\text{let } (x_1, x_2) = x \text{ in } q_{\Gamma, x_1: \tau_1, x_2: \tau_2}^\sigma(h)) \\
 &\quad \text{where } h(g, x_1, x_2) = f(g, (x_1, x_2))
 \end{aligned}$$

The base case is straightforward: the evaluation produces a closed value which can be inverted using the “quote” function of Definition 5.4. If the context includes a variable x of type \mathcal{Q}_1 , then we supply the only possible value for that variable (0), and inductively construct the term with the variable x bound to $()$. The result is of the correct type because we can add or drop bindings of variables of type \mathcal{Q}_1 to the environment. If the context includes a variable x of type \mathcal{Q}_2 , then we supply the two possible values for that variable 0 and 1. A conditional is then used to select the correct branch depending on the actual value of x . Finally, if the context includes a variable of type $\tau_1 \otimes \tau_2$

$\frac{}{\bullet \vdash \vec{0} : \sigma}$	$\frac{\Gamma \vdash t : \sigma}{\Gamma \vdash \kappa * t : \sigma}$	$\frac{\Gamma \vdash t, u : \sigma}{\Gamma \vdash t + u : \sigma}$
z-intro	prob	sup

Fig. 3. Typing quantum data (I)

then we simply flatten the product and proceed inductively. The function q_f^σ does indeed satisfy the inversion lemma.

6 Quantum Data and Control

We develop the typing rules and semantics of the quantum fragment of QML in two stages. First we extend the judgements $\Gamma \vdash t : \sigma$ and the semantics of Section 4 to handle quantum data in a straightforward manner. This simple treatment is only however an intermediate step in the development as it admits quantum programs that are not realisable on a quantum computer. We then refine both the type system and the semantics to identify exactly the realisable quantum programs.

6.1 The Category **Vec**

As a first approximation to a type system for QML programs, we consider the type system of Figure 1 extended with the rules in Figure 3.

Unlike the classical case, a judgement $\Gamma \vdash t : \sigma$ is *not* interpreted as a function in $\llbracket \Gamma \rrbracket \rightarrow \llbracket \sigma \rrbracket$. Rather, because we now have superpositions of terms with complex probability amplitudes, we interpret such judgements as functions in $\llbracket \Gamma \rrbracket \rightarrow \llbracket \sigma \rrbracket^{\mathbb{Q}}$ where $\llbracket \sigma \rrbracket^{\mathbb{Q}}$ represents the complex vectors over the base set $\llbracket \sigma \rrbracket$. In other words, $\llbracket \sigma \rrbracket^{\mathbb{Q}}$ is defined to be $\llbracket \sigma \rrbracket \rightarrow \mathbb{C}$ which is sometimes denoted $\mathbf{V} \llbracket \sigma \rrbracket$. We call the structure described above the category **Vec**.

Naturally this change requires that we revisit the semantics of the classical terms given in Figure 2 so that each denotation returns a complex vector. For example, we should have:

$$\llbracket \bullet \vdash \text{false} : \mathcal{Q}_2 \rrbracket^{\mathbb{Q}} = \text{const } v \quad \text{where } v \ 0 = 1 \text{ and } v \ 1 = 0$$

Instead of mapping the value representing the empty context to the denotation of false, we now return a vector v which associates the denotation of false with probability amplitude 1 and the denotation of true with probability amplitude 0.

This change can be done systematically by noticing that it corresponds to a monad whose unit and lift operation are defined below:

$$\text{return } a \ (b) = 1 \text{ if } a = b \text{ and } 0 \text{ otherwise}$$

$$f^*(v) = \sum a. (v \ a) * (f \ a)$$

More precisely every value that is returned in Figure 2 is explicitly tagged with the monadic *return* and when two functions are composed in Figure 2 using $f \circ g$, the composition is replaced by $f^* \circ g$.

$$\begin{array}{l}
 \llbracket \bullet \vdash \vec{0} : \sigma \rrbracket^Q = \text{const } v \text{ where } \forall a \in \llbracket \sigma \rrbracket. v \ a = 0 \\
 \llbracket \Gamma \vdash \kappa * t : \sigma \rrbracket^Q = g \quad \text{where } g \ a = \kappa * (f a) \\
 \quad \quad \quad f = \llbracket \Gamma \vdash t : \sigma \rrbracket^Q \\
 \llbracket \Gamma \vdash t + u : \sigma \rrbracket^Q = h \quad \text{where } h \ a = f \ a + g \ a \\
 \quad \quad \quad f = \llbracket \Gamma \vdash t : \sigma \rrbracket^Q \\
 \quad \quad \quad g = \llbracket \Gamma \vdash u : \sigma \rrbracket^Q
 \end{array}$$

Fig. 4. Meaning function for quantum data

The meaning of the new constructs for quantum data is given in Figure 4.

6.2 Orthogonality

The type system presented so far does indeed correctly track the uses of variables and prevents variables from being weakened; yet the situation is more subtle. It turns out that the type system accepts terms which implicitly perform measurements and as a consequence accepts programs which are not realisable as quantum computations.

Consider the expression **if**[°] x **then** $true$ **else** $true$: this expression appears, syntactically at least, to use x . However given the semantics of **if**[°], which returns a superposition of the branches, the expression happens to return $true$ without really *using* any information about x . In order to maintain the invariant that all measurements are explicit, the type system should reject the above expression as well.

More precisely, the expression **if**[°] x **then** t **else** u should only be accepted if t and u are *orthogonal* quantum values ($t \perp u$). This notion intuitively ensures that the conditional operator does not implicitly discard any information about x during the evaluation. Because of a similar concern, the two branches of a superposition should also be orthogonal.

The typing rules for conditionals and superpositions are modified as in Figure 5. This modification also achieves that programs are normalised, *i.e.*, the sum of the probabilities of a superposition add up to 1.

In Figure 6 we define the inner product of terms, which to any pair of terms $\Gamma \vdash t, u : \sigma$ assigns $\langle t | u \rangle \in \mathbb{C} \cup \{?\}$. This is used to define orthogonality: $t \perp u$ holds if $\langle t | u \rangle = 0$.

The judgement \vdash° is not automatically closed under the equality judgement, hence we add the rule (subst). Our philosophy is that we allow equivalent representations of QML programs which do not satisfy the orthogonality criteria locally, as long as the program as a whole is equivalent to one which does satisfy the criteria.

$$\boxed{
 \begin{array}{c}
 \frac{\Gamma \vdash^\circ c : \mathcal{Q}_2 \quad \Delta \vdash^\circ t, u : \sigma \quad t \perp u}{\Gamma \otimes \Delta \vdash^\circ \text{if}^\circ c \text{ then } t \text{ else } u : \sigma} \text{if}^\circ \\
 \frac{\Gamma \vdash^\circ t, u : \sigma \quad t \perp u \quad |\lambda|^2 + |\kappa|^2 = 1}{\Gamma \vdash^\circ \lambda * t + \kappa * u : \sigma} \text{sup}^\circ \\
 \frac{\Gamma \vdash^\circ t : \sigma \quad \Gamma \vdash t \equiv u : \sigma}{\Gamma \vdash^\circ u : \sigma} \text{subst}
 \end{array}
 }$$

Fig. 5. Typing quantum data (II)

$$\boxed{
 \begin{array}{ll}
 \langle t|t \rangle = 1 & \langle \lambda * t + \lambda' * t' | u \rangle = \lambda * \langle t|u \rangle + \lambda' * \langle t'|u \rangle \\
 \langle \text{false}|\text{true} \rangle = 0 & \langle t | \kappa * u + \kappa' * u' \rangle = \kappa * \langle t|u \rangle + \kappa' * \langle t|u' \rangle \\
 \langle \text{true}|\text{false} \rangle = 0 & \\
 & \langle \lambda * t|u \rangle = \lambda * \langle t|u \rangle \\
 \langle \vec{0}|\text{true} \rangle = 0 = \langle \text{true}|\vec{0} \rangle & \langle t|\lambda * u \rangle = \lambda \langle t|u \rangle \\
 \langle \vec{0}|\text{false} \rangle = 0 = \langle \text{false}|\vec{0} \rangle & \langle t + t'|u \rangle = \langle t|u \rangle + \langle t'|u \rangle \\
 \langle \vec{0}|x \rangle = 0 = \langle x|\vec{0} \rangle & \langle t|u + u' \rangle = \langle t|u \rangle + \langle t|u' \rangle \\
 \\
 \langle (t, t') | (u, u') \rangle = \langle t|u \rangle * \langle t'|u' \rangle & \langle t|u \rangle = ? \quad \text{otherwise}
 \end{array}
 }$$

Fig. 6. Inner products and orthogonality

6.3 The Category \mathbf{Q}°

The restriction of the set of typable terms requires a similar semantic restriction. All we need to do is to restrict the morphisms in the category of complex vectors to satisfy the following two conditions:

- **Linearity:** If $f \in \mathbf{V} A \rightarrow \mathbf{V} B$, $\alpha \in \mathbb{C}$, and $v, v_1, v_2 \in \mathbf{V} A$, then $f(v_1 + v_2) = f(v_1) + f(v_2)$ and $f(\alpha v) = \alpha(f v)$.
- **Isometry:** If $f \in \mathbf{V} A \rightarrow \mathbf{V} B$ and $v_1, v_2 \in \mathbf{V} A$, then $\langle v_1|v_2 \rangle = \langle f v_1|f v_2 \rangle$. (In other words, f preserves inner products of vectors.)

Two morphisms $f, g \in A \rightarrow B$ are *orthogonal* if for all vector $v \in \mathbf{V} A$, we have $\langle f v|g v \rangle = 0$. We call the resulting category, the category \mathbf{Q}° of strict quantum computations. The homset of morphisms in $[\Gamma] \rightarrow [\sigma]^\mathbf{Q}$ satisfying the above conditions is called $\mathbf{Q}^\circ [\Gamma] [\sigma]^\mathbf{Q}$.

The meaning function is given as before but with the maps interpreted in the category \mathbf{Q}° , *i.e.*, the meaning of a derivation $\Gamma \vdash t : \sigma$ is a morphism $[\Gamma \vdash t : \sigma]^\mathbf{Q} \in \mathbf{Q}^\circ [\Gamma] [\sigma]^\mathbf{Q}$. The requirement for orthogonality in the type system is reflected semantically: for isometries f, g , we have that $f|g$ is an

isometry, if f and g are orthogonal.

6.4 Quantum Equational Theory

The equational theory for the quantum language inherits all the equations for the classical case. This can be informally verified by noting that the meaning function in the case of the quantum language is essentially identical to the classical case. Formally, the proof technique explained in Section 4 applies equally well to the quantum case and yields the same equations for the classical core plus additional equations to deal with quantum data.

Definition 6.1 The *quantum equations* are:

(if[◦])

$$\begin{aligned} & \text{if}^\circ (\lambda * t_0 + \kappa * t_1) \text{ then } u_0 \text{ else } u_1 \\ \equiv & \lambda * (\text{if}^\circ t_0 \text{ then } u_0 \text{ else } u_1) + \kappa * (\text{if}^\circ t_1 \text{ then } u_0 \text{ else } u_1) \end{aligned}$$

(superpositions)

$$\begin{aligned} t + u & \equiv u + t \\ t + \vec{0} & \equiv t \\ t + (u + v) & \equiv (t + u) + v \\ \lambda * (t + u) & \equiv \lambda * t + \lambda * u \\ \lambda * t + \kappa * t & \equiv (\lambda + \kappa) * t \\ 0 * t & \equiv \vec{0} \end{aligned}$$

Lemma 6.2 (Soundness) *The equational theory is sound: if $\Gamma \vdash t \equiv u : \sigma$ then the isometries $\llbracket \Gamma \vdash t : \sigma \rrbracket^Q$ and $\llbracket \Gamma \vdash u : \sigma \rrbracket^Q$ are extensionally equal.*

The additional equations are used to prove equality between different quantum values. Semantically, two quantum values are the same if they denote the same vector, which is the case if the sum of the paths to each classical value is the same. For example, to find a simplified quantum value equivalent to:

$$(false + true) + (false + (-1) * true)$$

we first normalise to:

$$\begin{aligned} & (1 / \sqrt{2}) * ((1 / \sqrt{2}) * false + (1 / \sqrt{2}) * true) + \\ & (1 / \sqrt{2}) * ((1 / \sqrt{2}) * false + (-1 / \sqrt{2}) * true) \end{aligned}$$

This term has two paths to *false*; along each of them the product of the amplitudes is $(1 / \sqrt{2}) * (1 / \sqrt{2})$ which is $1 / 2$. The sum of all the paths to *false* is 1, and the sum of all the paths to *true* is 0. In other words, the entire term is equivalent to simply *false*. The above calculation proves that the Hadamard operation is self-inverse, as discussed in the introduction.

6.5 Quoting quantum values

We will now adapt the techniques developed in section 4 to the quantum case. A classical value $v \in \text{Val}^C \sigma$ is simply a term representing an element in $\llbracket \sigma \rrbracket$. A quantum value represents a vector in $\mathbf{V} \llbracket \sigma \rrbracket^Q$, hence we have to close values

under superpositions. We define $\text{Val}^Q \sigma \subseteq \text{Tm } \sigma$ inductively as a subset of closed terms of type σ :

- $\frac{v \in \text{Val}^C \sigma}{\text{val } v \in \text{Val}^Q \sigma}$
- $0 \in \text{Val}^Q \sigma$
- $\frac{v, w \in \text{Val}^Q \sigma}{v + w \in \text{Val}^Q \sigma}$
- $\frac{v \in \text{Val}^Q \sigma}{\kappa * v \in \text{Val}^Q \sigma}$

We write $\text{Val}_\circ^Q \sigma$ for isometric quantum values which satisfy the restrictions introduced in Figure 5.

We have already seen that there is a monadic structure on $\mathbf{V} A = A \rightarrow \mathbb{C}$. Correspondingly, we have a Kleisli structure on Val^Q ; $\text{val} \in \text{Val}^C \sigma \rightarrow \text{Val}^Q \sigma$ is the return and bind is defined as given $v \in \text{Val}^Q \sigma$ and $f \in \text{Val}^C \sigma \rightarrow \text{Val}^Q \tau$, we define $v \gg= f \in \text{Val}^Q \tau$ by induction over v :

$$\begin{aligned} (\text{val } x) \gg= f &= f \ x \\ 0 &\gg= f = 0 \\ v + w &\gg= f = (v \gg= f) + (w \gg= f) \\ \kappa * v &\gg= f = \kappa * (v \gg= f) \end{aligned}$$

Lemma 6.3 $(\text{Val}^C, \text{Val}^Q, \text{val}, (\gg=))$ is a Kleisli structure, i.e. it satisfies the following equations:

- (i) $\text{val } x \gg= f \equiv f \ x$
- (ii) $v \gg= \lambda x. \text{val } x \equiv v$
- (iii) $v \gg= \lambda x. (f \ x) \gg= g \equiv (v \gg= f) \gg= g$

Proof. Case (i) follows from the definition. Cases (ii) and (iii) can be shown by induction over the structure of v . \square

While the classical definition of q^σ (def. 5.4) was completely straightforward, its quantum counterpart is a bit more subtle, in particular the in the case of tensor products. As a special case consider $q^{\mathcal{Q}_2 \otimes \mathcal{Q}_2}$, given an element

$$\vec{v} \in [\![\mathcal{Q}_2 \otimes \mathcal{Q}_2]\!]^Q = [\![\mathcal{Q}_2]\!] \times [\![\mathcal{Q}_2]\!] \rightarrow \mathbb{C}$$

we have to construct a value $q^{\mathcal{Q}_2 \otimes \mathcal{Q}_2} \vec{v} \in \text{Val}^Q \mathcal{Q}_2 \otimes \mathcal{Q}_2$. This can be done by calculating the probabilities that the first qubit is i , $\text{fst } \vec{v} \ i \in \mathbb{R}^+$, given by

$$\text{fst } \vec{v} \ i = \sqrt{|\vec{v}(i, 0)|^2 + |\vec{v}(i, 1)|^2}$$

creating the first level of the value as a tree, and then for the second level normalising the amplitudes wrt. the probabilities of the previous level, see

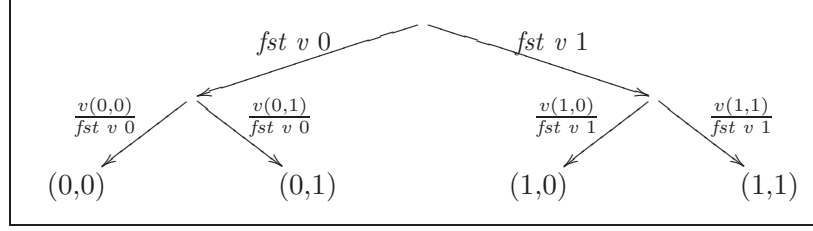

 Fig. 7. Value tree for $\mathcal{Q}_2 \otimes \mathcal{Q}_2$

figure 7 for the corresponding tree. We write $\llbracket \sigma \rrbracket^P = \llbracket \sigma \rrbracket \rightarrow \mathbb{R}^+$ for the set of probability distributions, obviously we have $\llbracket \sigma \rrbracket^P \subseteq \llbracket \sigma \rrbracket^Q$. We observe that $\text{fst } \vec{v} \in \llbracket \sigma \rrbracket^P$. Generalising the idea given above we arrive at the following definition of quote:

Definition 6.4 The *syntactic representations of denotations* is given by

$$q^\sigma \in \llbracket \sigma \rrbracket^Q \rightarrow \text{Val}^Q \sigma$$

defined by induction over σ :

$$q^{\mathcal{Q}_1} \vec{v} = (\vec{v} 0) * ()$$

$$q^{\mathcal{Q}_2} \vec{v} = (\vec{v} 1) * \text{true} + (\vec{v} 0) * \text{false}$$

$$q^{\sigma \otimes \tau} \vec{v} = q^\sigma(\text{fst } \vec{v})$$

$$\gg \lambda x \in \llbracket \sigma \rrbracket. (1/(\text{fst } \vec{v}) x) * q^\tau(\lambda y. \vec{v}(x, y))$$

$$\gg \lambda y. \text{val } (x, y)$$

where:

$$\text{fst} \in \llbracket \sigma \otimes \tau \rrbracket^Q \rightarrow \llbracket \sigma \rrbracket^P$$

$$\text{fst } \vec{v} x = \sqrt{\sum y. |\vec{v}(x, y)|^2}$$

$$1/- \in \llbracket \sigma \rrbracket^P \rightarrow \llbracket \sigma \rrbracket^P$$

$$1/\vec{v} x = \lambda x. \text{if } p x \equiv 0 \text{ then } 0 \text{ else } 1 / (p x)$$

To show adequacy we have to establish a number of properties of q^σ : we have to show that it is linear and isometric and that it preserves tensor products. This is summarised in the following proposition:

Proposition 6.5

- (i) $q^\sigma(\kappa * \vec{v}) \equiv \kappa * (q^\sigma \vec{v})$
- (ii) $q^\sigma(\vec{v} + \vec{w}) \equiv (q^\sigma \vec{v}) + (q^\sigma \vec{w})$
- (iii) $\langle \vec{v} | \vec{w} \rangle = \langle q^\sigma \vec{v} | q^\sigma \vec{w} \rangle$
- (iv) $q^{\sigma \otimes \tau}(\vec{v} \otimes \vec{w}) \equiv (q^\sigma \vec{v}, q^\tau \vec{w})$

The proof of the above proposition again isn't completely straightforward, e.g. linearity cannot just be proven by induction over σ . It is essential that

we first establish some properties of renormalising a vector wrt. a probability distribution. We define the product of a probability distribution $p \in \llbracket \sigma \rrbracket^P$ and a vector $\vec{v} \in \llbracket \sigma \rrbracket^Q$ as:

$$\begin{aligned} p * \vec{v} &\in \llbracket \sigma \rrbracket^Q \\ p * \vec{v} &= \lambda x \in \llbracket \sigma \rrbracket. (px) * (\vec{v} x) \end{aligned}$$

It is not hard to see that an analogous operation can be defined on values, given $v \in \text{Val}^Q \sigma$ and $p \in \llbracket \sigma \rrbracket^P$ as above, we define:

$$\begin{aligned} p * v &\in \text{Val}^Q \sigma \\ p * v &= v \gg \lambda x \in \llbracket \sigma \rrbracket. (px) * (\text{val } x) \end{aligned}$$

The key property we establish is

Lemma 6.6 *Given $p \in \llbracket \sigma \rrbracket^P$ and $\vec{v} \in \llbracket \sigma \rrbracket^Q$*

$$p * (q^\sigma \vec{v}) \equiv q^\sigma (p * \vec{v})$$

which can be verified by induction over σ and observing that while $1/-$ isn't a proper inverse, it nevertheless satisfies the following property

$$1/(p + q) * (p + q) = (1/p) * p$$

Using the fact that q^σ is isometric we can show that it produces values satisfying the orthogonality constraints:

Proposition 6.7 *Given $v \in \llbracket \sigma \rrbracket^Q$*

$$\vdash^\circ q^\sigma v : \sigma$$

6.6 Adequacy

We define a syntactic counterpart to:

$$\delta_{\Gamma, \Delta} \in \mathbf{Q}^\circ \llbracket \Gamma \otimes \Delta \rrbracket (\llbracket \Gamma \rrbracket^Q \otimes \llbracket \Delta \rrbracket^Q)$$

as:

$$\hat{\delta}_{\Gamma, \Delta} \in \text{Tm}(\Gamma \otimes \Delta) (|\Gamma| \otimes |\Delta|)$$

by:

$$\hat{\delta}_{\Gamma, \Delta} = \begin{cases} \text{let } (g, d) = \delta_{\Gamma', \Delta'} \text{ in } ((g, x), (d, x)) & \text{if } \Gamma = \Gamma', x : \sigma \\ & \text{and } \Delta = \Delta', x : \sigma \\ \text{let } (g, d) = \delta_{\Gamma', \Delta'} \text{ in } ((g, x), d) & \text{if } \Gamma = \Gamma', x : \sigma \\ & \text{and } x \notin \text{dom } \Delta \\ 1_\Delta & \text{if } \Gamma = \bullet \end{cases}$$

To establish that q^σ commutes with the context operations we have to show that contraction corresponds to $\delta \in \mathbf{Q}^\circ \llbracket \sigma \rrbracket (\llbracket \sigma \rrbracket^Q \otimes \llbracket \sigma \rrbracket^Q)$.

Lemma 6.8 *Given $v \in \llbracket \sigma \rrbracket^Q$ we have*

$$\mathbf{let} \ x = q^\sigma v \ \mathbf{in} \ (x, x) \equiv q^{\sigma \otimes \sigma} v$$

Proof. By induction on σ . □

Exploiting this property we can show that the context operations commute with quote:

Lemma 6.9 *Given $\vec{v} \in \llbracket \Gamma \otimes \Delta \rrbracket^Q$*

$$q^{|\Gamma| \otimes |\Delta|} (\delta_{\Gamma, \Delta} \vec{v}) \equiv \hat{\delta}_{\Gamma, \Delta} q^{|\Gamma \otimes \Delta|} \vec{v}$$

Theorem 6.10 *If $\Gamma \vdash t : \sigma$ and $g \in \llbracket \Gamma \rrbracket^Q$ then*

$$\vdash q^\sigma (\llbracket \Gamma \vdash t : \sigma \rrbracket^Q g) \equiv \mathbf{let}^* \Gamma = q^\Gamma g \ \mathbf{in} \ t : \sigma.$$

Proof. By induction over the derivation of $\Gamma \vdash t : \sigma$, as an example consider the case for let:

$$\begin{aligned} & q^\rho (\llbracket \Gamma \otimes \Delta \vdash \mathbf{let} \ x = t \ \mathbf{in} \ u : \rho \rrbracket^Q) \\ & \equiv \{ \text{definition of } \llbracket \cdot \rrbracket^Q \} \\ & q^\rho (\llbracket u \rrbracket^Q \circ (\llbracket t \rrbracket^Q \otimes id) \circ \delta_{\Gamma, \Delta}) \\ & \equiv \{ \text{induction hypothesis for } u \text{ and } t \} \\ & u \circ (t \circ q^\Gamma \otimes q^\Delta) \circ \delta_{\Gamma, \Delta} \\ & \equiv \{ \text{lemma 6.9} \} \\ & u \circ (t \otimes id) \circ \hat{\delta}_{\Gamma, \Delta} \circ q^{|\Gamma \otimes \Delta|} \\ & \equiv \\ & (\mathbf{let} \ x = t \ \mathbf{in} \ u) \circ q^{|\Gamma \otimes \Delta|} \end{aligned}$$

The other cases use the same style of reasoning to deal with the structural properties and exploit proposition 6.5. Note that the case for \mathbf{if}° can be reduced to linearity. □

Corollary 6.11 (Adequacy) *If $\vdash t : \sigma$ then $\vdash q^\sigma (\llbracket \vdash t : \sigma \rrbracket^Q) \equiv t : \sigma$*

6.7 Completeness and normalisation

The development here follows closely the one in the classical case as presented in Section 5.3.

Definition 6.12 The function:

$$q_\Gamma^\sigma \in \mathbf{Q}^\circ \llbracket \Gamma \rrbracket \llbracket \sigma \rrbracket^Q \rightarrow \mathbf{Tm} \ \Gamma \ \sigma$$

for *inverting evaluation* is defined by analysing the context:

$$\begin{aligned}
 q_{\bullet}^{\sigma}(f) &= q^{\sigma} (f \text{ (return 0)}) \\
 q_{\Gamma, x: \mathcal{Q}_1}^{\sigma}(f) &= \phi_{\Gamma, x: \mathcal{Q}_1}^{-1} \circ (q_{\Gamma}^{\rho}) \circ \Phi_{\Gamma, x: \mathcal{Q}_1} \\
 q_{\Gamma, x: \mathcal{Q}_2}^{\sigma}(f) &= \phi_{\Gamma, x: \mathcal{Q}_2}^{-1} \circ (q_{\Gamma}^{\sigma} \times q_{\Gamma}^{\sigma}) \circ \Phi_{\Gamma, x: \mathcal{Q}_2} \\
 q_{\Gamma, x: (\tau_1 \otimes \tau_2)}^{\sigma}(f) &= \phi_{\Gamma, x: \tau_1 \otimes \tau_2}^{-1} \circ q_{\Gamma, x_1: \tau_1, x_2: \tau_2}^{\sigma} \circ \Phi_{\Gamma, x: \tau_1 \otimes \tau_2}
 \end{aligned}$$

The auxiliary isomorphisms are defined as follows:

$$\begin{aligned}
 \phi_{\Gamma, x: \mathcal{Q}_1} &\in \text{Tm}(\Gamma, x : \mathcal{Q}_1) \sigma \rightarrow \text{Tm} \Gamma \sigma \\
 \phi_{\Gamma, x: \mathcal{Q}_1} t &= \text{let } x = () \text{ in } t \\
 \phi_{\Gamma} t &= t
 \end{aligned}$$

$$\begin{aligned}
 \phi_{\Gamma, x: \mathcal{Q}_2} &\in \text{Tm}(\Gamma, x : \mathcal{Q}_2) \sigma \rightarrow \{(t_0, t_1) \in (\text{Tm} \Gamma \sigma)^2 \mid t_0 \perp t_1\} \\
 \phi_{x: \mathcal{Q}_2} t &= (\text{let } x = \text{false in } t, \text{let } x = \text{true in } t) \\
 \phi_{\Gamma, x: \mathcal{Q}_2}^{-1}(t, u) &= \text{if}^{\circ} x \text{ then } t \text{ else } u
 \end{aligned}$$

$$\begin{aligned}
 \phi_{\Gamma, x: \tau_1 \otimes \tau_2} &\in \text{Tm}(\Gamma, x : \tau_1 \otimes \tau_2) \rho \rightarrow \text{Tm}(\Gamma, x_1 : \tau_1, x_2 : \tau_2) \\
 \phi_{\Gamma, x: \tau_1 \otimes \tau_2} t &= \text{let } x = (x_1, x_2) \text{ in } t \\
 \phi_{\Gamma, x: \tau_1 \otimes \tau_2}^{-1}(t) &= \text{let } (x_1, x_2) = x \text{ in } t
 \end{aligned}$$

The semantic map corresponding to each ϕ is written Φ .

For the inversion proof we only need the provability of one side of the isomorphisms which follows from the η -equalities.

Lemma 6.13 *The following family of equalities is derivable*

$$\phi_{\Gamma}^{-1}(\phi_{\Gamma} t) \equiv t$$

Definition 6.14 The *normal form* of t is given by $\text{nf}_{\Gamma}^{\sigma}(t) = q_{\Gamma}^{\sigma}(\llbracket \Gamma \vdash t : \sigma \rrbracket^{\mathcal{Q}})$.

Lemma 6.15 (Inversion) *The equation $\Gamma \vdash \text{nf}_{\Gamma}^{\sigma}(t) \equiv t$ is derivable.*

Proof. By induction over the definition of q_{Γ}^{σ} . In the case of $\Gamma = \bullet$ the result follows from adequacy, Corollary 6.11. In all the other cases we exploit Lemma 6.13. \square

Since all our definitions are effective nf indeed gives rise to a normalisation algorithm. As a consequence, our equational theory is decidable, modulo deciding equalities of the complex number terms which occur in our programs. We also note that as in the classical case, our theory is complete:

Proposition 6.16 (Completeness) *If $\llbracket \Gamma \vdash t : \sigma \rrbracket^{\mathcal{Q}}$ and $\llbracket \Gamma \vdash u : \sigma \rrbracket^{\mathcal{Q}}$ are extensionally equal, then we can derive $\Gamma \vdash t \equiv u : \sigma$.*

7 Conclusions and Further Work

We have developed a sound and complete equational theory for a functional quantum programming language, while at the same time providing a normalisation algorithm. The construction is a modular extension of a classical theory, indeed the quantum theory inherits not just all the equations and term formers, it is also possible to generalise our proof technique to the quantum case. The quantum theory introduces additional constructs corresponding to superpositions and equations relating them.

The obvious next step is to generalise this approach to the full language QML including measurements. The equational theory is already a challenge, since a measurement can have non-local effects on shared data. Semantically, we will be using superoperators to model programs with measurements. Clearly, we have to extend our quote operator to work on density matrices.

Another interesting direction, would be to consider higher order quantum programs and develop a complete equational theory and normalisation algorithm for this calculus. A likely semantic domain is given by presheaves, here the tensor product can be modelled using Day's construction, which is automatically closed, *i.e.*, provides an interpretation for higher types.

References

- [AD04] P. Arrighi and G. Dowek. Operational semantics for a formal tensorial calculus, 2004. Proceedings of the 2nd International Workshop on Quantum Programming Languages.
- [AG04] T. Altenkirch and J. Grattage. A functional quantum programming language. quant-ph/0409065, November 2004.
- [AU04] T. Altenkirch and T. Uustalu. Normalization by evaluation for λ^{-2} . In *Functional and Logic Programming*, number 2998 in LNCS, pages 260 – 275, 2004.
- [NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
- [Sel04] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 2004.
- [SV05] P. Selinger and B. Valiron. A lambda calculus for quantum computation with classical control. To appear in the proceedings of TLCA05, 2005.
- [vT03a] A. van Tonder. A lambda calculus for quantum computation. quant-ph/0307150, 2003. To appear in SIAM Journal of Computing.
- [vT03b] A. van Tonder. Quantum computation, categorical semantics and linear logic. quant-ph/0312174, 2003.